SysAdmin's Notebook

FortiGate Control of DLMS/COSEM Traffic

More devices, machines, and things are being networked these days than you can imagine; to the point that this trend in device communication is now encompassed by the term Internet of Things (IoT). Most people think that technological trend has to do with hooking up their smart fridge to the Internet so that it can tell them to pick up milk on the way home from work, but it really begins with Machine to Machine communication (M2M). M2M communication is already taking place because a lot of it is taking place in the industrial environment where it is not likely to be noticed, but it is vital to the infrastructure of the foundation of the modern world.

The term SCADA (Supervisory Control And Data Acquisition) is not often heard outside networking and technology circles, but it is becoming increasingly well known in the IT world. SCADA is the networking of the sensory and control mechanisms that are found in large systems. These systems often combine a large number of relatively simple technologies on a large-scale using an optimized method of control, such as a command center. They are found in everything from power plants to railways. A simple example of this technology would be a factory that makes widgets using an assembly line approach. Rather than having employees painstakingly inspect the mechanical components of a factory every hour, networked sensors and control devices can be installed to maintain a constant awareness of areas in need of monitoring or adjustment.

One of the specialized areas of SCADA is DLMS. Before going into how a FortiGate device can help protect DLMS traffic, it is good to have a thorough understanding DLMS.

What is DLMS/COSEM?

DLMS originally stood for Distribution Line Message Specification, though it was later changed to Device Language Message Specification. It is a model for communications at the Application layer between energy distribution devices in a computer integrated environment.

Closely related is COSEM, which is Companion Specification for Energy Metering. This includes specifications for both the Application and Transport layers. These two protocols are referred to as the DLMS/COSEM suite.

These protocols are used by:
- Utilities
- Manufacturers
- System Providers

For:
- Gas metering
- Water metering
- Electrical metering
- Heat metering

Controlling Access to DLMS/COSEM

Now that we have an idea of what DLMS/COSEM is, we can focus on how to manage DLMS/COSEM. If DLMS/COSEM traffic is going through your network, only certain devices should be communicating with each other using it. Protecting your network will not be about blocking the traffic, but controlling traffic. Even though the signatures are part of the IPS database, it is the Application Control profile that will be using the signatures.

Predefined Signatures

You can create your own custom signatures to govern the traffic, but a number of basic signatures have been created to protect traffic that involves the DLMS/COSEM protocol suite.The following signatures can be found in the FortiGate's **Application Control** section in the **Industrial** category:

```
DLMS.COSEM_Get.Request
DLMS.COSEM_Get.Response
DLMS.COSEM_Initiate.Request.High.Level.Authentication
DLMS.COSEM_Initiate.Request.Low.Level.Authentication
DLMS.COSEM_Initiate.Request.No.Authentication
DLMS.COSEM_Initiate.Response
DLMS.COSEM_Set.Request
DLMS.COSEM_Set.Response
Enabling the Signatures
```

Basic Application Control for the entire category

If you are looking for something basic and not very granular, like monitoring all of the signatures in the Industrial category, follow the steps below:

1. Go to **Security Profiles > Application Control**.
2. Select the Application Sensor that you wish to use.
3. In the **Categories** section, left-click on the **Industrial** category. The drop down menu will appear.
4. Choose the action that you want to apply to the entire category. Normally, most system administrators will start of with Monitor so that they can develop an idea of what the normal traffic of the category consists of. The actions available are the following: **Allow**, **Monitor**, **Block**, **Reset** or **Traffic Shaping**.
5. Select **Apply**.

Overriding Individual Signatures

After enabling basic application control for an entire category, you can apply more granular control for individual signatures. For example, if you have followed the steps above to block the Industrial category, you can now create an override to allow all DLMS/COSEM traffic in the category by following the steps below:

1. Go to the **Application Overrides** widget in the Edit Application Sensor window.
2. Select **Add Signatures**.
3. In the upper right Search field, enter `DLMS`.

4. From the results window, select and highlight the signatures that you wish to allow through. (Use the Shift key to select more than one at a time)
5. Select the **Use Selected Signatures** button.
6. Left click on the action of each of the signatures in the Action column and change it to the desired action. **Monitor** is preferable to **Allow**, in that it will allow you to keep track of when the traffic is going through.
7. Select **Apply.**
8. Apply the sensor to the profile that will govern the traffic.

IPS Database Information

The following information includes determining the latest IPS database, automatically updating your database, forcing an IPS update, and enabling extended IPS. It can also be found in the FortiOS handbook.

Verifying that you have the latest IPS database

To Determine the latest IPS Database:

1. Go to http://www.fortiguard.com/static/intrusionprevention.html
2. In the right of the page's menu bar is a button that starts "Latest IPS Database:" It will also have a version number. Clicking on the button will give you more information on that particular update of the database.
3. To determine which database you have use the CLI command:

```
get system auto-update versions
```

The relevant results will be similar to:

```
Attack Definitions
---------
Version: 5.00581
Contract Expiry Date: Sat Aug 15 2015
Last Updated using scheduled update on Sat Dec  6 04:51:28 2014
Last Update Attempt: Mon Dec  8 11:01:54 2014
Result: No Updates

Attack Extended Definitions
---------
Version: 5.00583
Contract Expiry Date: Sat Aug 15 2015
Last Updated using push update on Tue Dec  9 14:07:18 2014
Last Update Attempt: Thu Dec 11 13:19:30 2014
Result: No Updates
```

Automatically updating the IPS database

Are you set up to automatically update? This is the easiest method to make sure that the database is kept current. It does require a valid FortiGuard subscription.

Using the GUI:

1. Go to **System > Config > FortiGuard**.
2. At the bottom of the page, expand the **AV & IPS Download Options**.
3. Check **Scheduled Update**.

4. Choose the frequency for checking for updates. It can be done on an hourly, daily, or weekly basis. For the **Daily** and **Weekly** options the (hour) variable is to set to which hour of the day to run the checking procedure.
5. Click **Apply**.

Using the CLI
To get a quick, concise status of whether or not you are configured to automatically update the IPS database use the CLI command:

```
get system auto-update status
```

The results will be similar to the following:

```
FDN availability:  available at Thu Dec 11 13:19:30 2014
Push update:       enable
Push availability: available
Scheduled update: enable
Update daily: at 1 after 230 minutes
IPS definitions update: enable
Force an updating of the IPS database
```

Using the GUI
If you wish to force an update, you can use the Web based interface (GUI).

1. Go to **System > Config > FortiGuard**.
2. Down at the bottom of the page, expand the **AV & IPS Download Options**
3. Next to the **Scheduled Update** option is the **Update Now** button. Press this button and wait a few minutes for the process to complete.

Enabling the IPS Extended Database

It has not been discovered yet whether the DLMS signatures will be in the regular or the extended database. If they are in the extended database you will need to enable the extended database.

Using the GUI
Depending on the model, you may have the option to configure this in the GUI:

1. Go to **System > Config > FortiGuard**.
2. Down at the bottom of the page, expand the **AV & IPS Download Options.**
3. Check the box next to **Enable Extended IPS Signature Package**.

Using the CLI
If this option is not available you may be able to go into the CLI and run the commands:

```
config ips global
  set database extended
  end
```

Implementing DLMS/COSEM Application Control

Now that we know how to build the Application Control Sensor, we can use it with firewall objects and policies to create a network environment that allows only designated devices to communicate with the DLMS/COSEM enabled devices.

The first step will be to determine which network devices need to initiate DLMS/COSEM communications and which ones need to receive them. Address objects should be made for each and then address group objects should be made to include all of these objects.

DLMS/COSEM Application Control Example:

Group: “Building-2_MeterReaders"

Members: Water_Meter-1, Water_Meter-2, Gas_Meter-1,Gas_Meter-2, Electrical_Meter-1, and Electrical_Meter-2

Group: “Control_Systems"

Members: Local_Control_System and Off-site_Control_System

In this scenario, the **Building-2_MetreReaders** are all on one subnet off of port #5 and the traffic from **Control_Systems** will be coming through Port #1.

To control the traffic so that *only* DLMS/COSEM traffic from the **Control_Systems** reaches the **Building-2_MeterReaders** the following must be done:

1. The default Application Control Sensor being used on the policies from Port #1 to Port #5 must be edited so that it applies the **Block** action to the DLMS/COSEM signatures.
2. An Application Control Sensor must be created that applies the **Monitor** action to the DLMS/COSEM signatures. In this example, the sensor is named **DLMS-COSEM_open**.
3. Set your security policy to the following values:

Incoming Interface	Port #1
Source Address	**Control_Systems**
Outgoing Interface	Port #5
Destination Address	**Building-2_MeterReaders**
Action	ACCEPT
Application Control (ON)	**DLSM-COSEM_open**

4. Place the policy as close to the top of the policy sequence list as possible.

Any DLMS/COSEM traffic from the approved Control Systems going to the specified meter readers will be allowed by this policy. Any other DLMS/COSEM traffic will fall to subsequent policies which will be blocked.